TACKLE RANSOMWARE WITH LAYERED SECURITY

FOUR WAYS TO PREPARE YOU FOR THE VULNERABLE THREAT

There's no doubt that ransomware is an increasingly concerning threat in the IT industry. But you don't have to sit back and let it take over your data. Preventative measures and educated users are great first steps, but a layered approach to security will help minimize the ransomware risk.

WHAT IS RANSOMWARE?

Ransomware is a kind of malware which makes your corporate data and systems inaccessible. It does so by either locking PCs, or more commonly, encrypting the data that is practically unrecoverable–forcing the individual or organization to pay a ransom to regain access.

1) EMAIL AND WEB GATEWAY

As the first line of defense against ransomware, it's critical to protect the email and web gateway. Blocking at this point will protect the most vulnerable part of your organization–your users. Although ransomware attacks happen in many parts of your IT environment, the majority of ransomware attacks still come via email and web channels. If your user opens a malicious email attachment or clicks on a link that leads to a drive-by-download, it could have devastating consequences.

Trend Micro blocked 99 million ransomware threats between October 2015 and April 2016, and 99 percent of those threats were stopped at the gateway. If you catch ransomware at this stage, your users will never be exposed to the risk of clicking through.

Trend Micro™ Deep Discovery™ Email Inspector detects and blocks advanced spear phishing emails that bypass traditional filters.

Trend Micro Cloud App Security enhances your cloud-based email protection solutions. And although it has its own built-in security, it pays to have extra protection. Cloud App Security has blocked more than one million threats that weren't detected by Office 365. It has features like malware scanning and file risk assessment, sandbox malware analysis, document exploit detection, and web reputation.

Trend Micro™ InterScan™ Web Security stops users from visiting malicious or compromised sites. It features zero-day and browser exploit scanning, real-time web reputation to root out malicious URLs, and integration with Trend Micro™ Deep Discovery™ for advanced sandbox analysis.

2) ENDPOINT PROTECTION

Although 99 percent of threats were stopped by Trend Micro in the email and web gateway, that still leaves one percent that might sneak through. With one click of a mouse, your organization could be subjected to ransomware.

Trend Micro™ Smart Protection Suites™ have been architected to protect your users wherever they are: in the office, at home, on the road, or anywhere in between. Features like behavior monitoring, application control, vulnerability shielding, web reputation, and browser exploit protection work together to protect against the ransomware threat.

3) NETWORK DEFENSE

Although ransomware has traditionally been a consumer or end-user problem, criminal groups are now infiltrating ransomware into your network, causing every host, database, file share, and system backup to be exposed to the risk of being turned into an extortion engine.

Ransomware can enter your organization through any small part of your network that is undetected, which is why you need a clear sightline into network traffic, ports, and protocols across both physical and virtual segments of your network—you need a Network Defense strategy.

Trend Micro™ Deep Discovery Inspector™ delivers advanced detection, sandbox analysis, and integration with Trend Micro email and web gateways, endpoint, and server protection so you can gain clear visibility into everything going on in your network.

4) SERVER PROTECTION

Even if you have the email and web gateway covered, where most ransomware attacks occur, cybercriminals are now aiming straight for your servers—targeting unpatched vulnerabilities and out-of-support systems.

Server security is an essential part of the layered defense that organizations need to effectively mitigate the risk of ransomware.

Trend Micro™ Deep Security™ protects servers in physical, virtual, and cloud environments with host-based security. It includes multiple critical controls that can help stop ransomware from hitting your data center. It provides anti-malware scanning and web reputation, intrusion prevention (IPS), integrity monitoring, command and control (C&C) communication detection, and suspicious activity detection and prevention.

CENTRALIZED VISIBILITY AND CONTROL

As part of a layered defense strategy against ransomware, organizations should have multiple security controls in place across email, endpoints, networks, and servers.

Trend Micro™ Control Manager offers highly intuitive, centralized security visibility across all these layers from a single console, helping to reduce IT complexity and to stay on top of the ransomware threat.

The drill-down dashboard calls out where ransomware has shown up in the infection chain throughout your organization, including what was detected and how.

The timeline view shows ransomware detection over a period of time, and the single console simplifies administration and compliance reporting, freeing up time for other tasks.

SAY NO TO RANSOMWARE

No organization wants to deal with ransomware—not only is it costly, it can also have long-term effects on your organization. Just imagine your critical data being encrypted. By having a layered approach to security that is prioritized for the best risk mitigation, your organization can say no to ransomware.

Find out if your organization is ready for a ransomware attack. Get tips, preventative measures, and solutions to improve your ransomware security posture by visiting **ransomware-assessment.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud